CLAIMS

We claim:

1. A process for enrolling at least one personal identity credential into a personal identification device, wherein access to a personal identity credential is controlled by use of a biometric, comprising:
   a. producing a personal identification device, wherein a manufacturer maintains a database of a unique identifier and a unique public key for each personal identification device that it produces;
   b. distributing a public key possessed by said manufacturer to the personal identification device;
   c. creating an asymmetric key pair, comprising a private device key and a public device key, within the personal identification device;
   d. distributing the public key of the asymmetric key pair and a unique device identifier to the manufacturer;
   e. creating a first digital certificate containing the public key and the unique identifier;
   f. securely distributing the first digital certificate to the personal identification device;
   g. storing the public key and the unique identifier within the manufacturer's database;
   h. disabling all functionality of the personal identification device;
   i. requesting enrollment permission from an enrollment authority;
   j. validating the request for enrollment permission;
   k. presenting the first digital certificate to the enrollment authority;
   l. verifying that the personal identification device is the legitimate possessor of the first digital certificate;

m. presenting a second digital certificate possessed by the enrollment authority;

n. verifying that the enrollment authority is the legitimate possessor of the second digital certificate;

o. creating a symmetric session key; and

p. using the symmetric session key to securely transmit the personal identity credential and the associated biometric to the personal identification device.

2. The process of claim 1 further comprising the step of verifying that a digital signature accompanying the second digital certificate was signed by the manufacturer.

3. The process of Claim 1, further comprising securely archiving the personal identity credential, comprising the steps of:

a. creating a symmetric biometric encryption and decryption key;

b. encrypting a digital representation of the biometric with the symmetric biometric encryption and decryption key;

c. dividing the symmetric biometric encryption and decryption key into two unique and distinct parts;

d. encrypting the first part of the symmetric biometric encryption and decryption key with a user-specified passphrase;

e. creating a symmetric biometric digital signature associated with the second part of the symmetric biometric encryption and decryption key with the private key possessed by the personal identification device;

f. encrypting the second part of the symmetric biometric encryption and decryption key and the symmetric biometric digital signature with the public key possessed by the manufacturer of the personal identification device;

g. creating a symmetric personal identity credential encryption and decryption key;

h. creating a credential digital signature for the personal identity credential with the private key possessed by the personal identification device;

i. encrypting a digital representation of the personal identity credential and the credential digital signature with the symmetric personal identity credential encryption and decryption key;

j. dividing the symmetric personal identity credential encryption and decryption key into two unique and distinct parts;

k. encrypting the first part of the symmetric personal identity credential encryption and decryption key with a user-specified passphrase;

l. creating a symmetric personal identity digital signature associated with the second part of the symmetric personal identity credential encryption and decryption key with a private key possessed by the personal identification device;

m. encrypting the second part of the symmetric personal identity credential encryption and decryption key and the symmetric personal identity digital signature with a public key possessed by the manufacturer of the device;

n. storing the encrypted biometric, the signed and encrypted personal identity credential, the encrypted first and second parts of the symmetric biometric encryption and decryption key, and the encrypted first and second parts of the symmetric personal identity credential encryption and decryption key to a user-accessible electronic storage repository; and

o. releasing a digital certificate to a user associated with the personal identification device.

4. The process of claim 3, further comprising securely restoring the personal identity credential and the associated biometric to a secondary personal identification device, comprising the steps of:

a. obtaining the two encrypted, unique and distinct parts of the symmetric biometric encryption and decryption key;

b. decrypting the first part of the symmetric biometric encryption and decryption key with the user-specified passphrase;

c. decrypting the second part of the symmetric biometric encryption and decryption key and the symmetric biometric digital signature with a private key possessed by the manufacturer of the personal identification device;

d. verifying the symmetric biometric digital signature using the public key possessed by the personal identification device;

e. combining the two parts of the symmetric biometric encryption and decryption key;

f. decrypting the digital representation of the biometric using the symmetric biometric encryption and decryption key;

g. storing the digital representation of the biometric within the secondary personal identification device;

h. prompting a user to submit a new biometric to the secondary personal identification device, and authenticating the new biometric against the stored digital representation of the biometric;

i. obtaining the two digitally signed and encrypted, unique and distinct parts of the symmetric personal identity credential encryption and decryption key;

j. decrypting the first part of the symmetric personal identity credential encryption and decryption key with a user-specified passphrase;

k. decrypting the second part of the symmetric personal identity credential encryption and decryption key and the symmetric personal identity digital signature with a private key possessed by the manufacturer of the personal identification device;

l. combining the two parts of the symmetric personal identity credential encryption and decryption key;

m. decrypting the personal identity credential and the symmetric personal identity digital signature using the symmetric personal identity credential encryption and decryption key;

n. verifying the symmetric personal identity digital signature using a public key possessed by the personal identification device; and

o. storing the personal identity credential within the secondary device.

5. A method for providing means of future identification of a personal identification device, wherein access to a personal identity credential is controlled by use of a biometric, immediately following manufacturing of the device, comprising the steps of:

a. distributing a public key possessed by a manufacturer of the personal identification device to the personal identification device;

b. creating an asymmetric key pair, comprising a private device key and a public device key, within the personal identification device;

c. distributing the public device key of the asymmetric key pair and a unique device identifier to the manufacturer;

d. creating a digital certificate containing the public device key and the unique device identifier;

e. securely distributing the digital certificate to the personal identification device;

f. storing the public key and the unique identifier within a database; and

g. disabling all functionality of the personal identification device.

6. A method for securely enrolling at least one personal identity credential and an associated biometric into a personal identification device, wherein access to the personal identity credential is controlled by use of the biometric, comprising the steps of:

a. requesting enrollment permission from an enrollment authority;

b. validating the request for enrollment permission;

c. presenting a first digital certificate possessed by the personal identification device;

d. verifying that the personal identification device is the legitimate possessor of the first digital certificate;

e. presenting a second digital certificate possessed by the enrollment authority;

f. verifying that the enrollment authority is the legitimate possessor of the second digital certificate;

g. creating a symmetric session key; and

h. using the symmetric session key to securely transmit the personal identity credential and the associated biometric to the device.

7. The enrollment method of claim 6 further comprising the step of verifying that a digital signature accompanying the second digital certificate was signed by the manufacturer.

8. A method for securely archiving at least one personal identity credential pre-enrolled into an device with means for personal identification, wherein access to a personal identity credential is controlled by use of a biometric, comprising the steps of:
   a. creating a symmetric biometric encryption and decryption key;
   b. encrypting a digital representation of the biometric with the symmetric biometric encryption and decryption key;
   c. dividing the symmetric biometric encryption and decryption key into two unique and distinct parts;
   d. encrypting the first part of the symmetric biometric encryption and decryption key with a user-specified passphrase;
   e. creating a digital signature associated with the second part of the symmetric biometric encryption and decryption key with a private key possessed by the personal identification device;
   f. encrypting the second part of the symmetric biometric encryption and decryption key and the digital signature with a public key possessed by the manufacturer of the device;
   g. creating a symmetric personal identity credential encryption and decryption key,
   h. creating a digital signature for at least one personal identity credential with a private key possessed by the personal identification device;

i. encrypting the digital representation of at least one personal identity credential and the digital signature with the symmetric personal identity credential encryption and decryption key;

j. dividing the symmetric personal identity credential encryption and decryption key into two unique and distinct parts;

k. encrypting the first part of the symmetric personal identity credential encryption and decryption key with a user-specified passphrase;

l. creating a digital signature associated with the second part of the symmetric personal identity credential encryption and decryption key with a private key possessed by the personal identification device;

m. encrypting the second part of the symmetric personal identity credential encryption and decryption key and the digital signature with a public key possessed by the manufacturer of the device;

n. storing the encrypted biometric, and signed and encrypted personal identity credential, symmetric biometric encryption and decryption key, and symmetric personal identity credential encryption and decryption key to a user-accessible electronic storage repository; and

o. releasing a digital certificate to a user associated with the personal identification device, storing a unique identifier and a public key possessed by the personal identification device.

9. A method for securely restoring at least one personal identity credential and an associated biometric originally enrolled to a primary device with means for personal identification, pre-archived in a user-accessible electronic storage repository, to a secondary device with means for personal identification, wherein access to a personal identity credential is controlled by use of a biometric, comprising the steps of:
   a. obtaining two encrypted, unique and distinct parts of a symmetric biometric encryption and decryption key,
   b. decrypting the first part of the symmetric biometric encryption and decryption key with a user-specified passphrase,
   c. decrypting the second part of the symmetric biometric encryption and decryption key and an associated digital signature with a private key possessed by the manufacturer of the primary device,
   d. verifying the digital signature associated with the second part of the symmetric biometric encryption and decryption key using a public key possessed by the primary device,
   e. combining the two parts of the symmetric biometric encryption and decryption key,
   f. decrypting a digital representation of the biometric using the symmetric biometric encryption and decryption key,
   g. storing the digital representation of the biometric within the secondary device,
   h. prompting a user to submit a new biometric to the secondary device, and authenticating the new biometric against the stored biometric,
   i. obtaining two digitally signed and encrypted, unique and distinct parts of a symmetric personal identity credential encryption and decryption key,

j. decrypting the first part of the symmetric personal identity credential encryption and decryption key with a user-specified passphrase,

k. decrypting the second part of the symmetric personal identity credential encryption and decryption key with a private key possessed by the manufacturer of the primary device,

l. verifying the digital signature on the second part of the symmetric personal identity credential encryption and decryption key and an associated digital signature using a public key possessed by the primary device,

m. combining the two parts of the symmetric personal identity credential encryption and decryption key,

n. decrypting the personal identity credential and an associated digital signature using the symmetric personal identity credential encryption and decryption key,

o. verifying the digital signature associated with the personal identity credential using a public key possessed by the primary device, and

p. storing the personal identity credential appropriately within the secondary device.

10. A process for enrolling at least one personal identity credential into a personal identification device, wherein access to the at least one personal identity credential is controlled by use of an associated biometric, comprising:

assigning a unique identifier and a unique public key to the personal identification device;

maintaining a database of the unique identifier and the unique public key;

distributing a public key to the personal identification device;

creating an asymmetric key pair, comprising a private device key and a public device key, within the personal identification device;

transmitting the public device key of the asymmetric key pair and the unique identifier from the device;

creating a first digital certificate containing the public device key and the unique identifier;

securely distributing the first digital certificate to the personal identification device;

storing the public device key and the unique identifier within the database;

disabling all functionality of the personal identification device;

requesting enrollment permission from an enrollment authority;

validating the request for enrollment permission;

presenting the first digital certificate possessed by the personal identification device;

verifying that the personal identification device is the legitimate possessor of the first digital certificate;

presenting a second digital certificate possessed by the enrollment authority;

verifying that the enrollment authority is the legitimate possessor of the second digital certificate;

creating a symmetric session key; and

using the symmetric session key to securely transmit the personal identity credential and the associated biometric to the personal identification device.

11. The process of claim 10 further comprising the step of verifying a digital signature accompanying the second digital certificate was properly signed.

12. The process of claim 10, further comprising securely archiving the personal identity credential, comprising the steps of:

creating a symmetric biometric encryption and decryption key;

encrypting a digital representation of the biometric with the symmetric biometric encryption and decryption key;

dividing the symmetric biometric encryption and decryption key into two unique and distinct parts;

encrypting the first part of the symmetric biometric encryption and decryption key with a user-specified passphrase;

creating a symmetric biometric digital signature associated with the second part of the symmetric biometric encryption and decryption key with the private key possessed by the personal identification device;

encrypting the second part of the symmetric biometric encryption and decryption key and the symmetric biometric digital signature with the public key;

creating a symmetric personal identity credential encryption and decryption key;

creating a credential digital signature for the personal identity credential with the private key possessed by the personal identification device;

encrypting a digital representation of the personal identity credential and the credential digital signature with the symmetric personal identity credential encryption and decryption key;

dividing the symmetric personal identity credential encryption and decryption key into two unique and distinct parts;

encrypting the first part of the symmetric personal identity credential encryption and decryption key with a user-specified passphrase;

creating a symmetric personal identity digital signature associated with the second part of the symmetric personal identity credential encryption and decryption key with a private key possessed by the personal identification device;

encrypting the second part of the symmetric personal identity credential encryption and decryption key and the symmetric personal identity digital signature with a public key possessed by the manufacturer of the device;

storing the encrypted biometric, the signed and encrypted personal identity credential, the encrypted first and second parts of the symmetric biometric encryption and decryption key, and the encrypted first and second parts of the symmetric personal identity credential encryption and decryption key to a user-accessible electronic storage repository; and

releasing a digital certificate to a user associated with the personal identification device.

13. The process of claim 12, further comprising securely restoring the personal identity credential and the associated biometric to a secondary personal identification device, comprising the steps of:

obtaining the two encrypted, unique and distinct parts of the symmetric biometric encryption and decryption key;

decrypting the first part of the symmetric biometric encryption and decryption key with the user-specified passphrase;

decrypting the second part of the symmetric biometric encryption and decryption key and the symmetric biometric digital signature;

verifying the symmetric biometric digital signature using the public device key;

combining the two parts of the symmetric biometric encryption and decryption key;

decrypting the digital representation of the biometric using the symmetric biometric encryption and decryption key;

storing the digital representation of the biometric within the secondary personal identification device;

prompting a user to submit a new biometric to the secondary personal identification device, and authenticating the new biometric against the stored digital representation of the biometric;

obtaining the two digitally signed and encrypted, unique and distinct parts of the symmetric personal identity credential encryption and decryption key;

decrypting the first part of the symmetric personal identity credential encryption and decryption key with a user-specified passphrase;

decrypting the second part of the symmetric personal identity credential encryption and decryption key and the symmetric personal identity digital signature;

combining the two parts of the symmetric personal identity credential encryption and decryption key;

decrypting the personal identity credential and the symmetric personal identity digital signature using the symmetric personal identity credential encryption and decryption key;

verifying the symmetric personal identity digital signature using the public device key; and

storing the personal identity credential within the secondary personal identification device.

14. A method for providing means of future identification of a personal identification device, wherein access to a personal identity credential is controlled by use of a biometric, immediately following manufacturing of the device, comprising the steps of:

distributing a public key to the personal identification device;

creating an asymmetric key pair, comprising a private device key and a public device key, within the personal identification device;

distributing the public device key of the asymmetric key pair and a unique device identifier;

creating a digital certificate containing the public device key and the unique device identifier;

securely distributing the digital certificate to the personal identification device;

storing the public device key and the unique identifier within a database; and

disabling all functionality of the personal identification device.